

Appl. No.: 09/937,634
Arndt, dated November 24, 2005
Reply to Office Action of May 24, 2005

REMARKS / ARGUMENTS

Applicant hereby submits amendments for improving the clarity of the subject matter of the specification.

Specifically, the phrase "which is a sequence generating function" is inserted into line 23 of page 5 of the application to further define and thereby clarify the purpose of the pseudo random sequence generator and that the pseudo random sequence generator is for performing a sequence generating function as already described in lines 24-25 of page 5 of the application, where it is explained that two inputs k and v are accepted by the pseudo random sequence generator for obtaining a sequence s where $s=R(k, v)$ and where s is later for use as a secret key for producing a cipher text.

Applicant further submits that lines 9-10 of page 6 of the application discloses that an updated initial value v_i is obtain by applying $F()$ to obtain $v_i=F(v_{i-1})$. $F()$ as a function is further described in lines 19-20 of page 6 using $v_i=v_{i-1}+1$ and a cryptographic hash function as examples. These examples clearly highlight to a person having ordinary skill in the art that $F()$ is generally a hash function. Therefore, Applicant respectfully submits that the phrase " v_i using a hash function $F()$ where" is inserted into line 10 of page 6 of the application for imparting clarity to that portion of the application.

Applicant respectfully submits amendments to claims 1, 14, 24 and 37 for improving clarity thereof and to better define the first function and the second function. Specifically, each of claims 1, 14, 24 and 37 has been rewritten to clarify the interrelationships between means or steps that are set forth therein for achieving the desired results expressed with respect to the corresponding means or steps. Further explanations on the amendments are provided in the following response to the rejection of claims 1, 14, 24 and 37.

Applicant further submits that claims 3, 16, 26 and 39 are amended to improve clarity thereof. Specifically, each of claims 3, 16, 26 and 39 is amended to clarify that the limitation " $F()$ " is a hash function for updating the initial value v_i . Further explanations on the amendments are provided in the following response to the rejection of claims 3, 16, 26 and 39.

Additionally, Applicant respectfully submits that each of claims 7, 19, 30 and 42 has been amended to improve clarity thereof. Specifically, the claims 7, 19, 30 and 42 have been amended to explain and highlight that the limitation " $h()$ ". Further explanations on the

Appl. No.: 09/937,634
Amdt. dated November 24, 2005
Reply to Office Action of May 24, 2005

amendments are provided in the following response to the rejection of claims 7, 19, 30 and 42.

Applicant also hereby submits amendments to each of claims 5-6, 17-18, 28-29 and 40-41 for improving the clarity thereof. Specifically, the term "cryptographic pseudo random generator" has been amended to read "pseudo random generator" in each of claims 5, 17, 28 and 40 to rectify antecedence inconsistencies therein. Additionally, the term "pseudo random generator" has been amended to read "pseudo random sequence generator" in each of claims 5-6, 17-18, 28-29 and 40-41 for rectifying inconsistencies between the application and the claims 5-6, 17-18, 28-29 and 40-41.

Additionally, Applicant respectfully submits that each of claims 11-13, 21-23, 34-36 and 44-46 is amended to correct antecedent problems therein.

Applicant respectfully submits that no new matter is added in the amendments.

Rejections under 35 U.S.C. 112 for Claims 1, 14, 24 and 37

In the Office Action, Examiner rejects Applicant's invention as defined in claims 1, 14, 24 and 37 in relation to 35 U.S.C. 112, by explaining that steps c & d, with respect to claims 1 and 24, and steps b & c, with respect to claims 14 and 37, make the claims indefinite and unclear in that neither means or steps nor interrelationship of means or steps are set forth in these claims in order to achieve the desired results expressed in the limitations set forth with respect to the above means or steps. Primarily, Examiner explains that the claims are not clear because the application of the first function and second functions are not clearly defined.

Response to Rejections under 35 U.S.C. 112 for Claims 1, 14, 24 and 37

Claims 1, 14, 24 and 37 are amended to improve clarity thereof and to better define the first function and the second function. Specifically, each of claims 1, 14, 24 and 37 has been rewritten to clarify the interrelationships between means/steps that are set forth therein for achieving the desired results expressed with respect to the corresponding steps/means.

Specifically, Applicant respectfully submits that the "first function" has been amended to read "sequence generating function" and that the "second function" has been amended to read "high-speed cipher".

Applicant further draws the attention of Examiner to line 22 of page 5 of the application where a pseudo random sequence generator is described. The pseudo random sequence generator is a specific kind of sequence generating function for generating the segment key as described in each of amended claims 1, 14, 24 and 37.

Appl. No.: 09/937,634
Andt. dated November 24, 2005
Reply to Office Action of May 24, 2005

Additionally, Applicant submits that a high-speed cipher is described in line 3 of page 5 of the application. A person having ordinary skill in the art will recognise that the use of high-speed cipher forms an essential component or step of an encrypting or decrypting process. This further demonstrates the differences between the first and second functions of each of original claims 1, 14, 24 and 37 which are respectively the sequence generating function and the high-speed cipher in each of the amended claims 1, 14, 24 and 37. Furthermore, the use of the segment key in the high-speed cipher demonstrates the interrelationship between the sequence generating function and the high-speed cipher and their correlation with the first and second functions of original claims 1, 14, 24 and 37.

Therefore, reconsideration and withdrawal of the rejections to claims 1, 14, 24 and 37 are respectfully requested.

Rejections under 35 U.S.C. 112 for Claims 3, 16, 26 and 39

Examiner rejects claims 3, 16, 26 and 39 for not providing sufficient antecedent basis for the limitation " $F()$ " in the claims 3, 16, 26 and 39.

Response to Rejections under 35 U.S.C. 112 for Claims 3, 16, 26 and 39

Applicant respectfully submits that claims 3, 16, 26 and 39 are amended to improve clarity thereof. Specifically, each of claims 3, 16, 26 and 39 is amended to clarify that the limitation " $F()$ " is a hash function for updating the initial value v_i . The limitation " $F()$ " as a hash function is demonstrated and exemplified in line 20 of page 6 of the application for defining and thereby clarifying the characteristic of $F()$.

Therefore, reconsideration and withdrawal of the rejections to claims 3, 16, 26 and 39 are respectfully requested.

Rejections under 35 U.S.C. 112 for Claims 7, 19, 30 and 42

Examiner rejects claims 7, 19, 30 and 42 for not providing sufficient antecedent basis for the limitation " $h()$ " in the claims 7, 19, 30 and 42.

Response to Rejections under 35 U.S.C. 112 for Claims 7, 19, 30 and 42

Applicant respectfully submits that each of claims 7, 19, 30 and 42 has been amended to improve clarity thereof. Specifically, the claims 7, 19, 30 and 42 have been amended to explain and highlight that the limitation " $h()$ " is the keyed hash function $h()$ in corresponding claims 6, 18, 29 and 41. Therefore, Applicant respectfully submits that each of amended claims 7, 19, 30 and 42 overcomes the rejections of insufficient antecedent basis.

Appl. No.: 09/937,634
Arndt. dated November 24, 2005
Reply to Office Action of May 24, 2005

Therefore, reconsideration and withdrawal of the rejections to claims 7, 19, 30 and 42 are respectfully requested.

Rejections under 35 U.S.C. 112 for Claims 2, 4, 6, 8-10, 15, 18, 20, 25-27, 29, 31-33, 38, 41 and 43

Examiner rejects claims 2, 4, 6, 8-10, 15, 18, 20, 25-27, 29, 31-33, 38, 41 and 43 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Response to Rejections under 35 U.S.C. 112 for Claims 2, 4, 6, 8-10, 15, 18, 20, 25-27, 29, 31-33, 38, 41 and 43

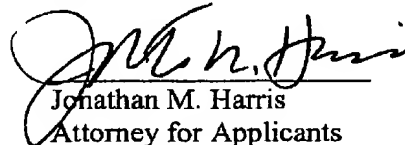
Applicant respectfully submits that each of claims 2, 4, 8-10, 15, 20, 25, 27, 31-33, 38 and 43 is directly or indirectly dependent on one of the amended claims 1, 3, 5-7, 11-14, 16-19, 21-24, 26, 28-30, 34-37, 39-42 and 44-46 for defining the subject matter therein. In light of Applicant's amendments and accompanying explanations to original claims 1, 3, 5-7, 11-14, 16-19, 21-24, 26, 28-30, 34-37, 39-42 and 44-46 to impart clarity and definitiveness to the indefinite elements therein, Applicant submits that claims 2, 4, 8-10, 15, 20, 25, 27, 31-33, 38 and 43 are now definite and that the subject matter therein is now clearly defined. Therefore, rejections to claims 2, 4, 8-10, 15, 20, 25, 27, 31-33, 38 and 43 are overcome and consequently fall away.

Reconsideration and withdrawal of the rejections to claims 2, 4, 8-10, 15, 20, 25, 27, 31-33, 38 and 43 are respectfully requested

CONCLUSION

Applicants respectfully request reconsideration and that a timely Notice of Allowance be issued in this case. Applicants believe a three month extension of time is needed and thus request the time extension. Please charge to Conley Rose, P.C.'s Deposit Account Number 03-2769/2085-00200.

Respectfully submitted,



Jonathan M. Harris
Attorney for Applicants
CONLEY ROSE, P.C.
P.O. Box 3267
Houston, Texas 77253-3267